Appendix E. Transition from Pilot to FNAL.GOV Realm (Sysadmin Information)

The production realm FNAL.GOV was launched on May 10, 2001. We are now transitioning to this realm from PILOT.FNAL.GOV. We expect the transition phase to end before October 31, 2001. In this appendix, we describe the things the administrator of a Kerberized system needs to know and do in order to complete the migration of the system from PILOT.FNAL.GOV to FNAL.GOV.

☞ The information in this chapter currently assumes that UNIX/Linux machines have the Fermi Kerberos product installed and Windows systems run WRQ® Reflection software.

E.1 Migrating your UNIX/Linux System’s Configuration to FNAL.GOV using UPD

As of June 5, Kerberos v1_3a is current in fnkits, as is krb5conf v1_4. Here are the steps for migrating to the production realm FNAL.GOV from the pilot realm. Use the latest version of Fermi kerberos available.

E.1.1 Quick Overview of Steps

First, to make your host aware of both realms and accessible by clients in either realm, issue the following commands on your system (using latest version of Fermi kerberos):

1) **`setup upd`**

2) **`upd install kerberos v1_x -G "-c"`**

3) **`ksu root`** [1]

4) **`ups install kerberos v1_x`**

5) **`ups add-new-realm kerberos`**

[1] In the root directory there must be a `.k5login` file with your principal listed for this to work.

The actions taken by **`ups add-new-realm kerberos`** are listed in section E.1.3 *The ups add-new-realm kerberos Action*. Then when you’re ready, change your default realm over to FNAL.GOV. To do so, issue the command:

1) **`ups change-realm kerberos`**

2) and send *nightwatch@fnal.gov* the full name of the host on which you’ve changed the default realm to FNAL.GOV.

☞ For machines on which Fermi kerberos is installed, but without host and FTP service keys, and hence no keytab file, this “change-realm” command will appear to fail when it can’t find `/etc/krb5.keytab`. Just ignore the “ABORT: keytab-convert failed” error, since the job is already done for you at that point. Or, you can just edit the `krb5.conf` file manually instead of running this command.

E.1.2 The Steps with More Detailed Information

1) Install the latest Fermi kerberos that is “current” in KITS. This will bring along the new krb5conf product.

2) After installation is complete, run the separate action **`ups add-new-realm kerberos`**. This will make your host aware of both realms and accessible by clients in either realm. Your system's default realm IS NOT CHANGED by this action. Details on what is changed are in section E.1.3 *The ups add-new-realm kerberos Action*.

3) You may want to run in this configuration for a while. You should be able to authenticate as *yourprincipal@FNAL.GOV* or as *yourprincipal@PILOT.FNAL.GOV* and have normal access to any other system on which steps 1 and 2 have also been performed.

4) When you’re ready to migrate your default realm to FNAL.GOV, execute **`ups change-realm kerberos`**. All this does is to change the default realm of the system to FNAL.GOV in `/etc/krb5.conf`, and to make sure the AFS servers are noted in that file as belonging to the same realm[1].

5) Send an email to *nightwatch@fnal.gov* listing the host(s) for which you’ve changed the default realm to FNAL.GOV.

[1] Actually, the AFS servers aren’t using Kerberos V5 at all yet, but for the Kerberos-to-AFS ticket/token translation, your host has to think it’s in the same realm as the AFS servers.

E.1.3 The ups add-new-realm kerberos Action

The following describes what is affected by the **`ups add-new-realm kerberos`** action. Note that as of kerberos version v1_3a this action is also available as two separate actions: migrate-keytabs and migrate-k5login.

1) The status of the krb5conf product is double-checked.

2) The new keytab-convert program is run on `/etc/krb5.keytab` and any cron keytabs found in `/var/adm/krb5`. If any key from the new realm is already present in the file, the program exits. Otherwise, the program duplicates every key in the old realm in the new realm. Before and after output of **`klist -k`** , in order, look like this[1]:

```
KVNO Principal
---- --------------------------------------------------
   3 ftp/gungnir.fnal.gov@PILOT.FNAL.GOV
   7 host/gungnir.fnal.gov@PILOT.FNAL.GOV
```

and

```
 KVNO Principal
---- --------------------------------------------------
    3 ftp/gungnir.fnal.gov@PILOT.FNAL.GOV
    7 host/gungnir.fnal.gov@PILOT.FNAL.GOV
    3 ftp/gungnir.fnal.gov@FNAL.GOV
    7 host/gungnir.fnal.gov@FNAL.GOV
```

3) For every home directory found in `/etc/passwd` or the NIS passwd map, if there is already a `.k5login` present, it is updated analogously to the keytab files. If the production realm (FNAL.GOV) is already mentioned, nothing happens. Otherwise, for every pilot realm principal mentioned in the file, the corresponding production realm principal is added. If the file is not readable and writable by the user in whose home directory it exists (perhaps because of AFS protection), it is skipped.

A couple of notes:

For host and FTP principals originally created in the pilot realm before May 10, this action puts the right FNAL.GOV realm key into the keytab file.

For projects (discussed in section) you have to run the keytab-convert program separately on the file defined as the project’s keytab.

[1] The KVNO (key version number) changes every time the key for a principal is changed. You may want to change a key to protect data. It is useful to know that, if a key is changed on a server while users are holding tickets issued on the old KVNO, the server can pick the right key to verify them. You can wait till all the current tickets expire, say 26 hours, then purge the old keys. A program to change keys may be available soon.

E.2 Migrating your UNIX/Linux System's Configuration to FNAL.GOV (no UPD)

E.2.1 Fermi Kerberos

Without UPS/UPD, but with Fermi Kerberos:

```
for i in /etc/krb5.conf /var/adm/krb5/??????????*; do
  /usr/krb5/bin/keytab-convert -v -o PILOT.FNAL.GOV -n FNAL.GOV $i
done
```

Then edit the `/etc/krb5.conf` default_realm under `[libdefaults]` and `[domain_realm]` info, as shown in Chapter 17: *The Kerberos Configuration File: krb5.conf*.

E.2.2 Non-Fermi Kerberos

With non-Fermi Kerberos and no UPD, request new passwords from *compdiv@fnal.gov* for host and ftp principals in FNAL.GOV realm only. Then run the following:

(`fqdn` means your host's fully qualified domain name, e.g., myhost@fnal.gov, or myhost@myuniv.edu)

```
for i in host ftp; do
  /usr/krb5/sbin/kadmin -r FNAL.GOV -p $i/$fqdn -q "ktadd $i/$fqdn"
  : (Supply password when requested)
done
```

Then edit the `/etc/krb5.conf` default_realm under `[libdefaults]` and `[domain_realm]` info, as shown in Chapter 17: *The Kerberos Configuration File: krb5.conf*.

E.3 Migrating your WRQ® (for Windows) Configuration to FNAL.GOV

Navigate to **START** > **PROGRAMS** > **REFLECTION** > **UTILITIES** > **KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application. Pull down the **CONFIGURATION** > **CONFIGURE REALMS...** menu, make sure the *Configuration* tab is selected.

1) Press **ADD**, and in the pop-up window, type FNAL.GOV for Realm, and `krb-fnal-1.fnal.gov` for KDC host.

2) Highlight the `FNAL.GOV` realm and click **PROPERTIES**.

3) With the *KDC* tab selected, press **ADD**, and in the pop-up window, type in the KDC host `krb-fnal-2.fnal.gov`. Click **OK** to add it to the *KDC list*. Repeat for the remaining FNAL.GOV realm KDCs (listed in section E.5 *KDC List*).

4) In the **KADMIN SERVER** box, replace the default value with `krb-fnal-admin.fnal.gov`.

☞ 5) Click the *Realm Defaults* tab and change the **PRE-AUTHENTICATION** from `None` to `Encrypted timestamp`. Click **OK**.

6) Set the default ticket lifetime to some non-zero value (26 hours is good).

7) Ignore the *Hosts* tab.

8) Now select the *Machine Defaults* tab and change the **DEFAULT TICKET LIFETIME** to 26 hours. Click **OK**.

9) Back on the **REFLECTION KERBEROS MANAGER** window, choose **CREDENTIALS**, then **NEW PRINCIPAL PROFILE...**

10) On the **ENTER PRINCIPAL** window, verify your principal name, and choose the realm FNAL.GOV. Click **OK**.

11) On the **CREATE NEW PRINCIPAL PROFILE** window, keep the default location for the credentials storage, and click **CREATE**.

12) Back on the **REFLECTION KERBEROS MANAGER** window, choose the tab with your new principal profile and check that your full FNAL.GOV principal is filled in.

E.4 Kerberized Client-Server Issues during Transition

E.4.1 How does a Client determine the Realm?

When a user invokes a Kerberized client program, the client program (e.g., Kerberized telnet, rsh, etc.) must decide which realm to ask for the service ticket. It bases this decision on (1) the hostname of the server for the client program, and (2) the rules which are now found in either or both of two places: the `[domain_realm]` sections of `/etc/krb5.conf` and `TXT` (text) records in DNS (the nameservers). The order in which these sources are tried for finding the realm of `somebox.fnal.gov` is[1]:

1) `somebox.fnal.gov = <REALM>` (in `krb5.conf`)

2) `_kerberos.somebox.fnal.gov txt <REALM>` (in DNS)

3) `.fnal.gov = <REALM>` (in `krb5.conf`)

4) `_kerberos.fnal.gov txt <REALM>` (in DNS)

[1] This determines the realm of the host/somebox.fnal.gov@<REALM> ticket that the client requests.

☞ Hosts which had service principals created before the realm migration began on May 10, 2001 have records matching number 2 in DNS, giving their realm as PILOT.FNAL.GOV, unless an email was sent to *nightwatch@fnal.gov* saying that the host's default realm has been changed. (See section D.5 *Finding out which Hosts have Migrated* for information on how to find the default realm of a given host.)

E.4.2 What if the Service Exists in Both Realms?

If the service actually exists in both realms, then for the case of telnet and the r-commands it doesn't matter which realm the client believes the server to be in, the server will have the necessary key to check the presented credentials. FTP, unfortunately, is written to a different API which hides the details of Kerberos from the application and makes it quite difficult for the application to accept credentials which treat the service as being in any realm other than the one to which the server host would map itself according to the rules above. If client and server are both relying on DNS for realm information, this will very rarely be a problem.

E.4.3 Migrated Client Hosts, Non-migrated Server Hosts

You may be running clients on your (migrated) system that commonly use servers on hosts that have not yet migrated to the production realm. This should present no problems for most clients. The telnet and r-command services will respond properly to clients who try to treat them as members of either realm, as long as the new kerberos and krb5conf products have been installed on the services' hosts.

However, an FTP server will accept Kerberos authentication only if the FTP client presents a service ticket from the service host's default realm[1]. To help out with that, the Kerberos code will now look for a DNS text record (or information in the `krb5.conf` file) for host-to-realm mapping information. This is discussed in section E.4.1 *How does a Client determine the Realm?*. Whenever *nightwatch@fnal.gov* is notified of a new host that's been migrated to FNAL.GOV, they will remove the explicit mapping of the host to the PILOT.FNAL.GOV realm from DNS. By this action, Kerberos is forced to look at the `.fnal.gov = <REALM>` line in the host's `krb5.conf` (or `_kerberos.fnal.gov txt REALM` in DNS) to determine the realm mapping, which will point to FNAL.GOV for this situation.

E.4.4 Resolving Host Name when Requesting a Service Ticket

A service name includes the full, official name of the server host (e.g., service/hostname.fnal.gov@REALM). Aliases or nicknames of the server host are resolved before requesting the service ticket. But if there is a hosts file

[1] The underlying requirement is that the server map its own name to the same realm to which the client maps the server's name.

or NIS map on the client machine that takes precedence over DNS, you might come up with the wrong name. Common errors include listing the “short” or one-word name or a nickname before the full name in a hosts file. This causes a request for a ticket for a service principal that usally does not exist in the Kerberos database.

E.5 KDC List

As of July 18, 2001, the current KDC nodes are listed below. For WRQ, note that the :88 should be left off.

For PILOT.FNAL.GOV

(Note the absence of “2”.)

krb-pilot-1.fnal.gov:88

krb-pilot-3.fnal.gov:88

krb-pilot-4.fnal.gov:88

krb-pilot-admin.fnal.gov (the master KDC for PILOT.FNAL.GOV)

For FNAL.GOV:

krb-fnal-1.fnal.gov:88

krb-fnal-2.fnal.gov:88

krb-fnal-3.fnal.gov:88

krb-fnal-4.fnal.gov:88

krb-fnal-5.fnal.gov:88

krb-fnal-6.fnal.gov:88

krb-fnal-admin.fnal.gov (the master KDC for FNAL.GOV)